IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION FOR PATENT

METHOD, APPARATUS AND SYSTEM FOR SECURELY PROVIDING MATERIAL TO A LICENSEE OF THE MATERIAL

Inventor: David C. Collier

CROSS REFERENCE TO RELATED APPLICATION

This application is related to co-pending Provisional Patent Application Serial No. 60/346802 which is incorporated herein by reference in its entirety.

FIELD OF THE INVENTION

The present invention generally relates to techniques for preventing unauthorized use of material and in particular, to a method, apparatus and system for securely providing material to a licensee of the material.

BACKGROUND OF THE INVENTION

Providers of material demand compensation for the use of their material or content. Unauthorized use cheats these providers of their due compensation. Therefore, techniques for preventing such unauthorized use have been and continue to be developed. As soon as new techniques are developed and practiced, however, dishonest users seek to circumvent those techniques to avoid paying compensation to the content providers. Consequently, techniques for preventing unauthorized use of material evolve to stay one step ahead.

OBJECTS AND SUMMARY OF THE INVENTION

Accordingly, it is an object of the present invention to provide a method for securely providing material to a licensee of the material.

Another object is to provide an apparatus for securely providing material to a licensee of the material.

Still another object is to provide a system for securely providing material to a licensee of the material.

These and additional objects are accomplished by the various aspects of the present invention that uses at least a two-key approach for added security. Briefly stated, one aspect is a method for securely providing material to a licensee of the material that includes providing at least one license key to a licensee of material; providing the material encrypted with at least one content key to the licensee; and providing the at least one content key encrypted with the at least one license key to the licensee.

Another aspect is an apparatus for securely providing material to a licensee of the material. The apparatus includes at least one server that is configured to transmit at least one license key to a client device operable by a licensee of material; transmit the material encrypted with at least one content key to the client device; and transmit the at least one content key encrypted with the at least one license key to the client device.

Another aspect is a system for securely providing material to a licensee of the material. The system includes a client device operable by a licensee of material; and at least one server configured to transmit at least one license key, the material encrypted with at least one content key,

and the at least one content key encrypted with the at least one license key to the client device.

Still another aspect is a method for securely providing material to a licensee of the material that includes providing a license to use material and a license key corresponding to the license; providing the material encrypted with a content key; and providing the content key encrypted with the license key.

Yet another aspect is a method for securely providing material to a licensee of the material that includes receiving a license to use material and a license key corresponding to the license; receiving the material encrypted with a content key; receiving the content key encrypted with the license key; decrypting the encrypted content key using the license key; and decrypting the encrypted material using the decrypted content key.

Additional objects, features and advantages of the various aspects of the present invention will become apparent from the following description of its preferred embodiments, which description should be taken in conjunction with the accompanying drawings.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. 1 illustrates a flow diagram of a method implemented, for example, by one or more servers for securely providing material to a licensee of the material, utilizing aspects of the present invention.

FIG. 2 illustrates a flow diagram of a method implemented, for example, by a client for securely providing material to a licensee of the material, utilizing aspects of the present invention.

FIGS. 3~4 illustrate, as examples, block diagrams of three systems for securely providing material to a licensee of the material, utilizing aspects of the present invention.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENT

As used herein: the terms "audio-visual content" or "A/V content" includes audio, visual and other multimedia content including motion pictures, music, the spoken word, photos, and printed text; "material" and "content" may be used interchangeably, and includes A/V and other distributed content such as computer programs or software; and "proprietary material" means material protected by contract or intellectual property law.

FIG. 1 illustrates, as an example, a flow diagram of a method for securely providing material to a licensee of the material that may be performed by one or more servers. In **101**, a content or material request is received from a client. The client in this case may be a person, or a client device such as a computer, a set-top box, network appliance, wireless communicating device such as a personal digital assistant ("PDA") or other type of electronic device. Along with the content request that identifies the content being requested such as, for example, a movie or music title, information identifying a client device or its operator may also be provided. In the case of the client device, this may take the form of a host or network interface card identification number, and in the case of the operator, this may take the form of a credit card number or user identification and password. For establishing secure communications between electronic devices, a public key "KU" may also be provided along with the content request. In such

case, a conventional authentication and key exchange procedure may be performed to establish a secure channel.

In **102**, the transaction is authorized in a conventional manner. Preferably this takes the common form of verifying that the requester or operator of the client has properly paid for the requested content and is not otherwise prohibited from receiving it. Payment may be by credit card with conventional bank confirmation. In addition, the requester may also be first required to accept terms of a license agreement in a click-the-button or other conventional manner before the transaction is authorized.

In **103**, a license detailing the usage rights purchased by the requester is provided to the client. The usage rights may include many conventional items such as the number of allowed viewings or playing of material such as a movie, music recording, electronic book, entertainment event or software program. They may also include such things as the time period over which such viewings or playing is allowed. U.S. Pat. No. 5,715,403 entitled "System for Controlling the Distribution and Use of Digital Works having Attached Usage Rights where the Usage Rights are defined by a Usage Rights Grammar", which is incorporated in its entirety herein by this reference, gives numerous examples of such usage rights.

In **104**, at least one license key "KL" corresponding to the license is provided preferably at the same time as the license to the client. As will be discussed in more detail below, a primary purpose of the at least one license key "KL" is to provide a second level of security by encrypting an at least one content key "KC" that is in turn, used to encrypt the requested content prior to its transmission to the client. In one embodiment of the invention, the at least one

license key comprises a plurality of license keys that are used one-at-a-time in a predetermined fashion for encrypting the at least one content key.

In **105**, the at least one content key "KC" is conventionally generated. In **106**, the at least one content key is encrypted by the at least one license key in a conventional manner. Where the at least one license key comprises a plurality of license keys for encrypting and decrypting the at least one content key, the plurality of license keys are preferably used one-at-a-time in a predetermined fashion for such encryption and corresponding decryption. For example, they may be used on a periodically rotating time basis for encrypting and decrypting the at least one content key. Thus, with the many possible combinations of license and content keys, increased security is provided using the method.

In **107**, the requested material is encrypted with the at least one content key "KC" in a conventional manner. Where the at least one content key comprises a plurality of content keys for encrypting and decrypting the requested material, the plurality of content keys are preferably used one-at-a-time in a predetermined fashion for such encryption and corresponding decryption, depending upon the application. In **108**, the content key encrypted with the license key (also referred to herein simply as the "encrypted content key") and the material encrypted with the at least one content key (also referred to herein simply as the "encrypted material" or "encrypted content") are provided to the client, either in separate transactions or in the same transaction. The order of the separate transactions is generally not important. The encrypted material may be provided as a file or streaming media.

In one application example where the requested content or material is included in at least one MPEG-4 bit stream such as its video and audio bit streams, the at least one content key conventionally comprises a plurality of content keys that are used one-at-a-time in a predetermined fashion for encrypting corresponding time periods of the material. Alternatively, they may be used one-at-a-time in a predetermined fashion for encrypting corresponding portions of the material. The at least one content key in this case is encrypted with the at least one license key, and included in an IPMP ("Intellectual Property Management & Protection") stream that is provided to the licensee along with the material included in the MPEG-4 bit stream that is encrypted with the at least one content key. The at least one content key in this case is conventionally mapped to corresponding portions of the material included in the at least one MPEG-4 bit stream that is encrypted with the at least one content key, by IPMP descriptors associated with the corresponding portions.

FIG. 2 illustrates, as an example, a flow diagram of a method for securely providing material to a licensee of the material that may be performed by a client and is complementary to the method described in reference to **FIG. 1**. In **201**, a content or material request is made by a client. The client in this case may be a person, or a client device such as a computer, a set-top box, network appliance, wireless communicating device such as a PDA or other type of electronic device. Along with the content request that identifies the content being requested such as, for example, a movie or music title, information identifying a client device or its operator may also be provided. In the case of the client device, this may take the form of a host or network interface card identification number, and in the case

of the operator, this may take the form of a credit card number or user identification and password. For establishing secure communications between electronic devices, a public key "KU" may also be provided along with the content request. In such case, a conventional authentication and key exchange procedure may be performed to establish a secure channel, thus providing a third level of security through three key levels (i.e., KU, KL and KC).

In **202**, a license detailing the usage rights purchased by the requester is received. In **203**, at least one license key "KL" corresponding to the license is also received, either along with the license or in a separate transaction. In **204**, the requested material is received encrypted with at least one content key. In **205**, the at least one content key "KC" is received encrypted with the at least one license key, either along with the encrypted material or in a separate transaction. When the encrypted material and the encrypted at least one content key are received in separate transactions, the order that they are received is generally not important. When the encrypted at least one content key is provided with the encrypted material, such as in the case of the MPEG-4 example described above, the encrypted at least one content is extracted from the combination.

In **206**, the encrypted at least one content key is decrypted using the at least one license key in a conventional manner. Where the at least one content key comprises a plurality of content keys, and/or the at least one license key comprises a plurality of license keys, such decryption generally follows a complementary process to the encryption described in reference to **106** of **FIG. 1**. In **207**, the encrypted content or material is then decrypted using the

at least one content key in a conventional manner. Where the at least one content key comprises a plurality of content keys, such decryption generally follows a complementary process to the encryption described in reference to **107** in **FIG. 1**. In **208**, the content is then used in accordance with the license, using conventional control software installed on the client device. The at least one license key in such case may also be used in certain applications to effectively activate the license so that it may be used with the control software.**FIGS. 3~4** illustrate, as examples, block diagrams of representative systems for securely providing material to a licensee of the material. In **FIG. 3**, a server **301** performs the method described in reference to **FIG. 1**, and a client **302** performs the method described in reference to **FIG. 2**. In this case, all transmissions between the server **301** and the client **302** go through a communication medium **303**, which may be, for examples, the Internet or a direct connection through cable, satellite, digital subscriber line ("DSL") or other telephone modem.

In **FIG. 4**, a server **401** likewise performs the method described in reference to **FIG. 1**, and a client **402** likewise performs the method described in reference to **FIG. 2**. In this case, however, certain portions of the methods described in reference to **FIGS. 1** and **2**, such as, for example, the content request and transmission of the encrypted content and encrypted at least one content key, go through a communication medium **403**, and other portions of the methods described in reference to **FIGS. 1** and **2**, such as, for example, the transmission of the license and the license key, go through another communication medium **404** for additional security.

In **FIG. 5**, servers **501** and **503** combine to perform the method described in reference to **FIG. 1**, whereas client **502** performs the method described in reference to **FIG. 2**. In this system, the server **501** is referred to as a content or data providing server, because it preferably performs portions of the method described in reference to **101**, **102** and **105~108** in **FIG. 1**. The server **503**, on the other hand, is referred to as a license server, because it preferably performs the remaining portions of the method described in reference to **103** and **104** in **FIG. 1**. Other arrangements of multi-server systems are also fully contemplated to be within the full scope of the present invention. U.S. Pat. No. 6,202,056 B1 entitled "Method for Computer Network Operation Providing Basis for Usage Fees", which is incorporated in its entirety herein by this reference, is just one example of a multi-server system in which the present invention may be employed.

Although the various aspects of the invention have been described with respect to preferred embodiments, it will be understood that the invention is entitled to full protection within the full scope of the appended claims.